

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**STIPULATION OF  
EXPECTED TESTIMONY**

**Mr. Peter Artale**

9 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Peter Artale were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am currently employed by the Army Counter-Intelligence Center (ACIC) with the 902d Military Intelligence Group on Fort Meade, Maryland. ACIC produces finished intelligence products for the intelligence community. It often produces these products by fulfilling requests for information from the Army. It takes finished products and disseminates them on SIPRNET and JWICS. I am a Web Developer and the Team Lead of a team of three software developers. I have worked in this capacity and for ACIC for eight years. Prior to this position, I worked in web development for the Defense Intelligence Agency (DIA) for one year, then with Booz Allen on a one year contract with National Geo-Spatial Agency. I was a software development engineer and programmer in the Air Force for twenty-one years. I retired from the Air Force as a Master Sergeant. I also have an Associate's degree in Computer Science.

2. I first became involved in this case on approximately 17 March 2010 after my Branch Chief, Ms. Jessica Johnson, alerted me to the compromise of U.S. Government information. Ms. Johnson asked if I could use our system to see who had viewed a certain product. I could, as I had developed custom software to track access to particular products. This software captures the viewer credentials by recording the Internet Protocol (IP) address and date/time of access for each user who views our ACIC work product. It then assigns a unique report key to the access event. This occurred before we were contacted by law enforcement in this case, as ACIC was notified of the compromise of one of our products in March 2010.

3. An IP address is part of the Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol is the standard language used to communicate over a network. TCP/IP is the most common "language" that computers use to communicate over the Internet. And so, an IP address is the method of identifying a specific computer on a network. Only one computer can be assigned a specific IP address at one time. Knowing an IP address allows us to know which computer on a given network used our products. Our software is a custom product which, in capturing this user and access information, produces metrics which can be used to see which of our products are most popular and how our products are used. The software only logged views of the document in the ".asp" format which is the standard way the product would appear on the website. ".asp" is a common file format for web pages. This means that the software only logged views of the web version of the document and not the views of the ".pdf" or ".doc" version of the document. Likewise, the logs do not indicate whether the document was printed or saved, nor do they indicate how long an individual looked at the document, if at all. We

collect this data normally so we can analyze it to see where we need to allocate our development and maintenance resources to best support our internal and external customers. The information produced by the tracking software is, therefore, called metrics.

4. The metrics are pulled when an engineer runs a certain query. These queries can be customized to pull only the information the developer wants to see. In this case, we were specifically interested in tracking every access to a product titled "WikiLeaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorists Groups?" Therefore, I searched the product by determining and searching for its product identification number, which is "RB08-0617". The product identification number, which is on the document itself and assigned internally by ACIC, is a identifier unique to each ACIC product.

5. This ACIC product "WikiLeaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorists Groups?" is housed on our website at "acic.north-inscom.army.smil.mil" and is accessible only via a classified network, such as SIPRNET. I wrote a custom query, by IP address and visit time, to see every time this particular document was pulled from the web server. A custom query is a method of pulling information from a database. I pulled these metrics from my own workstation. The data is automatically pulled into a Structured Query Language (SQL) table. SQL is a computer language for extracting and inserting information in a database. It is a standard computer language to interact with databases. Printouts of SQL queries look like an excel spreadsheet in that it has columns and rows; however, it is not as easy to search and organize as an excel spreadsheet. I, therefore, digitally cut and pasted the information from the SQL table into an excel spreadsheet and saved the data to my desktop. I then organized the spreadsheets in two separate manners. The first set is organized by visit date. The second is organized by IP address and then visit date. I did not alter the content of the data in any way when searching for the data, moving it from the SQL table to the excel spreadsheet, or while in the excel spreadsheet. I moved the information and organized it in two separate manners because it was easier to read. I then emailed the metric data to my leadership at ACIC as requested. The data is stored securely on our servers and is only accessible to the other three web developers on my team. I have no reason to believe anyone else would have modified the logs in any way. This occurred before we were contacted by investigators involved in this case, as ACIC was notified of the compromise of one of our products in March 2010.

6. In this case, the ACIC document concerned was posted in 2008. I pulled the metric data tracking access to this document on 17 March 2010. The most recent access date listed in the metric data is 16 March 2010. The data returned included view hits on the document up until the morning I ran the data query. The logs are broken down by record key, IP address, and visit date. Specifically, the metrics tell me the following about the user IP addresses who opened the website containing the product with a product identification number of RB08-0617 in the web page format: a user with the IP address 22.225.41.40 opened the web page on 1 December 2009 at 6:31 PM; a user with the IP address 22.225.41.40 opened the web page on 29 December 2009 at 2:40 PM; a user with the IP address 22.225.41.40 opened the web page on 1 March 2010 at 6:40 PM; and a user with the IP address 22.225.41.22 opened the web page on 7 March 2010 at 11:31 PM.

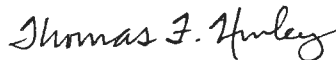
7. The data for these metrics is collected by our custom software automatically when someone clicks on one of our links to use our ACIC work product. This system captures the time, date, and IP address as well as which product is being accessed and served out to the requester. We know this data is accurate because there is no human intervention into the process and because views are logged using specific codes and for specific products. Finally, while it is possible to make manual insertions in metric data output, those insertions cannot be backdated or overwritten. This means whatever output data the system produces cannot itself be altered. Furthermore, at the time I pulled these logs, I did not know to whom the IP addresses were attached or the reasons for which the data was being pulled. I had neither the motivation nor knowledge required to alter the document. At no point prior to pulling the metric log data, while pulling the information, or after securing it, did I ever alter the data in any way.

8. My Branch Chief forwarded my email with these metrics to Mr. Winston Budram, S-6 and Chief Information Officer of the 902d MI Group. Mr. Budram forwarded the metrics to investigators after they contacted our office. **Prosecution Exhibit (PE) 63 for Identification** is the paper copy of these logs. **PE 63 for ID** is a printout of the complete logs that I pulled. I put the title "Views of ACIC Product RB08-0617.asp" on the top of the excel spreadsheet. The title is based on the ACIC product identification number and the format of the document. On the left side of every page are the logs that I pulled and organized by visit date. On the right side of every page are the logs that I pulled and organized by IP Address and then visit date. I believe the information on the top of the page ("Views of ACIC Product RB08-0617.asp"; "Record Key"; "IP Address"; and "Visit Date"), which is the same as the title and heading information on the spreadsheets that I pulled, was automatically produced by excel when the spreadsheets were printed.

9. I am the custodian of the records marked as **PE 63 for ID** and an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities. **PE 63 for ID** was made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters. **PE 63 for ID** was kept in the course of regularly conducted business activity. It was the regular practice of the business activity to make the records. The records marked as **PE 63 for ID** are a true, accurate, and complete copy of the original documents.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel



THOMAS HURLEY  
MAJ, JA  
Defense Counsel



BRADLEY E. MANNING  
PFC, USA  
Accused